Canad. Math. Bull. Vol. **60** (4), 2017 pp. 774–790
http://dx.doi.org/10.4153/CMB-2016-084-8

On the Structure of the Schild Group in Relativity Theory

Gerd Jensen and Christian Pommerenke

Abstract. Alfred Schild has established conditions that Lorentz transformations map world-vectors (ct, x, y, z) with integer coordinates onto vectors of the same kind. These transformations are called integral Lorentz transformations.

This paper contains supplements to our earlier work with a new focus on group theory. To relate the results to the familiar matrix group nomenclature, we associate Lorentz transformations with matrices in $\mathrm{SL}(2,\mathbb{C})$. We consider the lattice of subgroups of the group originated in Schild's paper and obtain generating sets for the full group and its subgroups.

1 Introduction

1.1 Notations

Let $\mathbb{Z}[\mathrm{i}]$ be the ring of Gaussian integers $m + \mathrm{i}n$ with $m, n \in \mathbb{Z}$. The function $\pi\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{Z}_2$, defined by $\pi(m + \mathrm{i}n) = 0$ if m and n are both even or both odd and $\pi(m + \mathrm{i}n) = 1$ otherwise, is a ring homomorphism; $\pi(w)$ is called the *parity* of w. If $\pi(w) = 0$, then w is called *even*, otherwise *odd*. Using $2 = (1 + \mathrm{i})(1 - \mathrm{i})$, one concludes that w is even if and only if it is divisible by $(1 + \mathrm{i})$.

Let $\mathrm{M}(2,\mathbb{C})$ and $\mathrm{M}(2,\mathbb{Z}[\mathrm{i}])$ be the rings of 2×2-matrices with components in $\mathbb{C}$ and $\mathbb{Z}[\mathrm{i}]$, respectively, and $\mathrm{SL}(2,\mathbb{C}) = \{A \in \mathrm{M}(2,\mathbb{C}) : \det A = 1\}$. The symbols a, b, c, d will always denote the components of

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}(2,\mathbb{C}).$$

Let $\|A\|^2 := |a|^2 + |b|^2 + |c|^2 + |d|^2$. For $A \in \mathrm{SL}(2,\mathbb{C})$, we have $\|A^{-1}\|^2 = \|A\|^2$.

Further we set

$$\omega = \frac{1+\mathrm{i}}{2}, \quad \rho = \frac{1+\mathrm{i}}{\sqrt{2}}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E := \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \tag{1.1}$$

$$T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -\mathrm{i} & 0 \\ 0 & 1 & \mathrm{i} & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}.$$

Received by the editors September 4, 2016.
Published electronically May 16, 2017.
AMS subject classification: **22E43**, 20H99, 83A05.
Keywords: Lorentz transformation, integer lattice, Gaussian integers, Schild group, subgroup.

The matrix T is unitary. Let

$$L_A := T^*(\overline{A} \otimes A)T, \tag{1.2}$$

where ⊗ denotes the Kronecker product. The expanded form is ([4])

$$L_A = \begin{pmatrix} \frac{1}{2}(|a|^2+|b|^2+|c|^2+|d|^2) & \operatorname{Re}(a\overline{b}+c\overline{d}) & -\operatorname{Im}(a\overline{b}+c\overline{d}) & \frac{1}{2}(|a|^2-|b|^2+|c|^2-|d|^2) \\ \operatorname{Re}(a\overline{c}+b\overline{d}) & \operatorname{Re}(a\overline{d}+b\overline{c}) & -\operatorname{Im}(a\overline{d}-b\overline{c}) & \operatorname{Re}(a\overline{c}-b\overline{d}) \\ \operatorname{Im}(a\overline{c}+b\overline{d}) & \operatorname{Im}(a\overline{d}+b\overline{c}) & \operatorname{Re}(a\overline{d}-b\overline{c}) & \operatorname{Im}(a\overline{c}-b\overline{d}) \\ \frac{1}{2}(|a|^2+|b|^2-|c|^2-|d|^2) & \operatorname{Re}(a\overline{b}-c\overline{d}) & -\operatorname{Im}(a\overline{b}-c\overline{d}) & \frac{1}{2}(|a|^2-|b|^2-|c|^2+|d|^2) \end{pmatrix}. \tag{1.3}$$

Evidently

$$L_{uA} = L_A \quad \text{for } |u| = 1, \text{ in particular } L_{-A} = L_A. \tag{1.4}$$

From the properties of the Kronecker product it follows that $A \mapsto L_A$ is a ring homomorphism $\mathrm{M}(2,\mathbb{C}) \to \mathrm{M}(4,\mathbb{R})$ and

$$\det L_A = 1 \quad \text{for } |\det A| = 1. \tag{1.5}$$

Hence $A \mapsto L_A$ is a group homomorphism $\{A \in \mathrm{M}(2,\mathbb{C}) : |\det A| = 1\} \to \mathrm{SL}(4,\mathbb{R})$.

1.2 Schild's Theorem

The elements of the ring $\mathrm{M}(4,\mathbb{Z})$ will be called *integral*. Schild's main theorem [8] characterized the integral matrices of the form L_A (see [4, Theorem 1.1]).

Theorem 1.1 (Schild) *Let $A \in \mathrm{M}(2,\mathbb{C})$ and $|\det A| = 1$. Then $L_A \in \mathrm{M}(4,\mathbb{Z})$ if and only if there is $u \in \mathbb{C}$ with $|u| = 1$ such that $B := uA$ satisfies $\det B \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$, and one of the following.*

(i) *$B \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}])$ and $\|B\|^2$ even.*
(ii) *$B \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E$.*

The theorem describes $\mathbf{S}^* := \{A \in \mathrm{M}(2,\mathbb{C}) : |\det A| = 1, L_A \in \mathrm{M}(4,\mathbb{Z})\}$. By (1.5), $\mathbf{S}^*$ is the inverse image of $\mathrm{SL}(4,\mathbb{Z})$ in the group $\{A \in \mathrm{M}(2,\mathbb{C}) : |\det A| = 1\}$ under the homomorphism $A \mapsto L_A$ and therefore a group. It is not required that $A \in \mathrm{SL}(2,\mathbb{C})$. The weaker condition $|\det A| = 1$ is in line with the proof of Theorem 1.1 where it leads to comparatively few case distinctions. On the other hand, from (1.4) it follows that $\{L_A : |\det A| = 1\} = \{L_A : \det A = 1\}$, so the same set of transformations L_A is gathered under the condition $\det A = 1$ as under $|\det A| = 1$. However, removing redundancies by limiting the scope to $\mathrm{SL}(2,\mathbb{C})$ provides a better insight into the group structure and discloses relations to familiar subgroups of $\mathrm{SL}(2,\mathbb{C})$. In Section 2 we will therefore reformulate Theorem 1.1 and study

$$\mathbf{S} := \{A \in \mathrm{SL}(2,\mathbb{C}) : L_A \in \mathrm{M}(4,\mathbb{Z})\}. \tag{1.6}$$

By (1.5), $\mathbf{S}$ is the inverse image of $\mathrm{SL}(4,\mathbb{Z})$ in $\mathrm{SL}(2,\mathbb{C})$ under the homomorphism $A \mapsto L_A$ and therefore also a group.

Definition 1.2 $\mathbf{S}$ shall be called the *Schild group*.

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

1.3 Relation to the Lorentz Transformations

The Lorentz group $\mathrm{O}(1,3)$ consists of the linear transformations of $\mathbb{R}^4$ which preserve the quadratic form $t^2 - x^2 - y^2 - z^2$ (the speed of light is assumed to be 1). Schild's concern was to determine which elements of $\mathrm{O}(1,3)$ map $\mathbb{Z}^4$ onto itself. Using the common identification of linear transformations with their coefficient matrices, this amounts to the determination of $\mathrm{O}(1,3) \cap \mathrm{M}(4,\mathbb{Z})$, since the matrices in $\mathrm{O}(1,3)$ are unimodular. This is the group of *integral Lorentz transformations*. From the outset Schild simplified the task utilizing the following facts.

- The Lorentz transformations preserving both the direction of time and the orientation of space make up the subgroup $\mathrm{SO}^+(1,3) \subset \mathrm{SL}(4,\mathbb{R})$ of *restricted* Lorentz transformations. Every element of $\mathrm{O}(1,3)$ is a product of an element of $\mathrm{SO}^+(1,3)$ and one or both of the diagonal matrices $\operatorname{diag}(1,-1,-1,-1)$ and $\operatorname{diag}(-1,1,1,1)$. Therefore it is sufficient to characterize the elements of $\mathrm{SO}^+(1,3) \cap \mathrm{M}(4,\mathbb{Z})$.
- The homomorphism $A \mapsto L_A$ produces a double cover of $\mathrm{SO}^+(1,3)$ by $\mathrm{SL}(2,\mathbb{C})$ (see for instance [1, Sec. 6.3]), hence
$$\mathrm{SO}^+(1,3) \cap \mathrm{M}(4,\mathbb{Z}) = \{L_A : A \in \mathrm{SL}(2,\mathbb{C}), L_A \in \mathrm{M}(4,\mathbb{Z})\}.$$
If (1.6) is written as $\mathbf{S} = \{A : A \in \mathrm{SL}(2,\mathbb{C}), L_A \in \mathrm{M}(4,\mathbb{Z})\}$, it becomes obvious that
$$\mathrm{SO}^+(1,3) \cap \mathrm{M}(4,\mathbb{Z}) = \{L_A : A \in \mathbf{S}\}.$$
It is therefore sufficient to study integral transformations of the form L_A.
- The linear transformation of $\mathbb{R}^4$ brought about by L_A can be replicated by one of $\mathbb{C}^2$ in virtue of the equivalence
$$(1.7)\quad L_A(t,x,y,z)^\intercal = (t',x',y',z')^\intercal \iff A\begin{pmatrix} t+z & x+\mathrm{i}y \\ x-\mathrm{i}y & t-z \end{pmatrix}A^* = \begin{pmatrix} t'+z' & x'+\mathrm{i}y' \\ x'-\mathrm{i}y' & t'-z' \end{pmatrix},$$
see [4]. This reduces a problem about 16 real components with 10 constraints down to one with 4 complex components subject to only one (complex) constraint.

1.4 Overview

In Section 2 we introduce the subclasses of $\mathbf{S}$ necessary for a reformulation of Schild's theorem and derive various relations among them that are needed in Section 3 for the investigation of subgroups of $\mathbf{S}$ and their cosets. With a method originally advised by H. S. M. Coxeter (see [8, Appendix]) and later used by Lorente and Kramer [5, §2], we derive in Section 4 generators for the groups dealt with in Section 3, thus also providing a systematic way to produce integer matrices which satisfy the Lorentzian orthogonality relations. A different approach was presented by Louck who used the theory of Diophantine equations to develop algorithms for the construction of integral Lorentz transformations [6]. In Section 5 we give an example of an integral Lorentz transformation that cannot be decomposed into an integral rotation and an integral boost. In Section 6 the relation of the subgroup of integral Gaussian matrices in $\mathbf{S}$ to the group of all integral Gaussian matrices in $\mathrm{SL}(2,\mathbb{C})$ is discussed.

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

2 Subclasses of S

2.1 Primary Subdivision

The numbers ρ and ω were defined in (1.1). The following theorem is the announced modification of Theorem 1.1, already mentioned in Schild's paper.

Theorem 2.1 *The group* **S** *is the union of the pairwise disjoint sets*

$$\begin{aligned} \mathbf{G} &:= \{A \in \mathrm{SL}(2,\mathbb{C}) : A \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) \text{ and } \|A\|^2 \in 2\mathbb{Z}\}, \\ \mathbf{H} &:= \{A \in \mathrm{SL}(2,\mathbb{C}) : A \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E\}, \\ \mathbf{V} &:= \{A \in \mathrm{SL}(2,\mathbb{C}) : A \in \rho\, \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) \text{ and } \|A\|^2 \in 2\mathbb{Z}\}, \\ \mathbf{W} &:= \{A \in \mathrm{SL}(2,\mathbb{C}) : A \in \rho(\mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E)\}. \end{aligned} \tag{2.1}$$

Proof Let $A \in \mathrm{SL}(2,\mathbb{C})$. By Theorem 1.1 we have $A \in \mathbf{S}$ if and only if there is $u \in \mathbb{C}$, $|u| = 1$, such that $B := uA$ satisfies $\det B = \mathrm{i}^k = \rho^{2k}$ for some $k \in \{0,1,2,3\}$. Hence

$$1 = \rho^{-2k} \det B = \det(\rho^{-k}B) = \det(u\rho^{-k}A) = (u\rho^{-k})^2 \det A = (u\rho^{-k})^2,$$

and one of the following cases takes place.

- $B \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}])$ and $\|\rho^{-k}B\|^2 = \|B\|^2$ is even: Then

$$u\rho^{-k}A = \rho^{-k}B \in \begin{cases} \mathbf{G} & \text{if } k \text{ is even,} \\ \mathbf{V} & \text{if } k \text{ is odd.} \end{cases}$$

  Hence from $u\rho^{-k} = \pm 1$, $\mathbf{G} = -\mathbf{G}$, and $\mathbf{V} = -\mathbf{V}$, it follows that $A \in \mathbf{G}$ or $A \in \mathbf{V}$.
- $B \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E$: Since $\omega \mathrm{i}^l E = \omega(\mathrm{i}^l - 1)E + \omega E \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E$, we have

$$u\rho^{-k}A = \rho^{-k}B \in \begin{cases} \mathrm{i}^l(\mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E) \in \mathbf{H} & \text{if } k \text{ is even and } k = -2l, \\ \rho\mathrm{i}^l(\mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) + \omega E) \in \mathbf{W} & \text{if } k \text{ is odd and } k = -2l-1. \end{cases}$$

  Hence from $u\rho^{-k} = \pm 1$, $\mathbf{H} = -\mathbf{H}$, and $\mathbf{W} = -\mathbf{W}$, it follows that $A \in \mathbf{H}$ or $A \in \mathbf{W}$. ■

For later reference we note that

$$\mathbf{G}^{-1} = \mathbf{G}, \quad \mathbf{H}^{-1} = \mathbf{H}, \quad \mathbf{V}^{-1} = \mathbf{V}, \quad \mathbf{W}^{-1} = \mathbf{W}. \tag{2.2}$$

We also add a more manageable definition for **G**; an analogous statement is true for **V**, but we do not need it.

Lemma 2.2 *Each of the following lines is equivalent to* (2.1)*:*

$$\mathbf{G} = \{A \in \mathrm{SL}(2,\mathbb{C}) : A \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) \text{ and } a+b+c+d \text{ even}\}, \tag{2.3}$$

$$\mathbf{G} = \{A \in \mathrm{SL}(2,\mathbb{C}) : A \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}]) \text{ and } a+b, c+d, a+c, b+d \text{ odd}\}. \tag{2.4}$$

Proof The equivalence of (2.1) and (2.3) follows from

$$\begin{aligned} \pi(|a|^2 + |b|^2 + |b|^2 + |b|^2) &= \pi(a)\pi(\overline{a}) + \pi(b)\pi(\overline{b}) + \pi(c)\pi(\overline{c}) + \pi(d)\pi(\overline{d}) \\ &= \pi(a)^2 + \pi(b)^2 + \pi(c)^2 + \pi(d)^2 \\ &= \pi(a) + \pi(b) + \pi(c) + \pi(d) = \pi(a+b+c+d). \end{aligned}$$

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

If A satisfies the conditions in (2.3), then $a+b$ and $c+d$ are both odd or both even. The latter is impossible because of $1 = ad - bc = (a+b)d - b(c+d)$. The analogous result holds for the column sums, so A satisfies the conditions in (2.4). Conversely, if the conditions in (2.4) are fulfilled, then those in (2.3) also hold. ∎

2.2 Refinement

If $A \in \mathbf{H}$, then the sum of any two of its components is in $\mathbb{Z}[\mathrm{i}]$, and if $A \in \mathbf{W}$, then the sum of any two of its components is in $\rho\mathbb{Z}[\mathrm{i}]$.

Lemma 2.3 (i) *If $A \in \mathbf{H}$, then $a+b+c+d$ is even.*
(ii) *If $A \in \mathbf{W}$, then $(a+b+c+d)/\rho$ is even.*

Proof (i) Let $a = a' + \omega$, $b = b' + \omega$, $c = c' + \omega$, $d = d' + \omega$ with $a', b', c', d' \in \mathbb{Z}[\mathrm{i}]$. Then

$$\begin{aligned} 1 = ad - bc &= a'd' - b'c' + \omega(a' + d' - b' - c') = a'd' - b'c' + \omega(a + d - b - c) \\ &= a'd' - b'c' - (1+\mathrm{i})(b+c) + \omega(a+b+c+d). \end{aligned}$$

Since $1/\omega = 1 - i$, we deduce that $a+b+c+d = (1-\mathrm{i})(1 - a'd' + b'c') + 2(b+c)$.

(ii) Let $a/\rho = a' + \omega$, $b/\rho = b' + \omega$, $c/\rho = c' + \omega$, $d/\rho = d' + \omega$ with $a', b', c', d' \in \mathbb{Z}[\mathrm{i}]$. Then

$$\begin{aligned} 1 = ad - bc &= \rho^2(a'd' - b'c' + \omega(a' + d' - b' - c')) \\ &= \mathrm{i}(a'd' - b'c' + \omega(a + d - b - c)/\rho) \\ &= \mathrm{i}(a'd' - b'c') - \mathrm{i}(1+\mathrm{i})(b+c)/\rho + \mathrm{i}\omega(a+d+b+c)/\rho. \end{aligned}$$

Since $1/(\mathrm{i}\omega) = -(1+i)$, we deduce that

$$(a+b+c+d)/\rho = -(1+\mathrm{i})(1 - \mathrm{i}(a'd' - b'c')) + 2(b' + c' + 1 + \mathrm{i}). \qquad ∎$$

By Lemma 2.3, for $A \in \mathbf{H}$, the row sums $a+b$ and $c+d$ are both even or both odd, and the analogous statement holds for the column sums. Similarly, for $A \in \mathbf{W}$, the sums $(a+b)/\rho$ and $(c+d)/\rho$ are both even or both odd, and the same holds for $(a+c)/\rho$ and $(b+d)/\rho$. Let

$$\begin{aligned} &\mathbf{H}^0 := \{A \in \mathbf{H} : \text{row sums even}\}, && \mathbf{W}^0 := \{A \in \mathbf{W} : (\text{row sums})/\rho \text{ even}\}, \\ &\mathbf{H}^1 := \{A \in \mathbf{H} : \text{row sums odd}\}, && \mathbf{W}^1 := \{A \in \mathbf{W} : (\text{row sums})/\rho \text{ odd}\}, \\ &\mathbf{H}_0 := \{A \in \mathbf{H} : \text{column sums even}\}, && \mathbf{W}_0 := \{A \in \mathbf{W} : (\text{column sums})/\rho \text{ even}\}, \\ &\mathbf{H}_1 := \{A \in \mathbf{H} : \text{column sums odd}\}, && \mathbf{W}_1 := \{A \in \mathbf{W} : (\text{column sums})/\rho \text{ odd}\}. \end{aligned}$$

This defines two partitions of $\mathbf{H}$ and of $\mathbf{W}$:

$$\text{(2.5)} \qquad \mathbf{H} = \mathbf{H}^0 \dot\cup \mathbf{H}^1 = \mathbf{H}_0 \dot\cup \mathbf{H}_1, \quad \mathbf{W} = \mathbf{W}^0 \dot\cup \mathbf{W}^1 = \mathbf{W}_0 \dot\cup \mathbf{W}_1.$$

Supplementing (2.2), we also note that

$$\text{(2.6)} \qquad (\mathbf{H}_0)^{-1} = \mathbf{H}^0, \ (\mathbf{H}_1)^{-1} = \mathbf{H}^1, \quad (\mathbf{W}_0)^{-1} = \mathbf{W}^0, \ (\mathbf{W}_1)^{-1} = \mathbf{W}^1.$$

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

Next we introduce two matrices $P \in \mathbf{H}$ and $Q \in \mathbf{V}$ which will serve as paradigms and important tools:

$$(2.7)\quad P := \begin{pmatrix} \overline{\omega} & \overline{\omega} \\ -\omega & \omega \end{pmatrix} = \begin{pmatrix} (1-\mathrm{i})/2 & (1-\mathrm{i})/2 \\ -(1+\mathrm{i})/2 & (1+\mathrm{i})/2 \end{pmatrix} = -\begin{pmatrix} \mathrm{i} & \mathrm{i} \\ 1+\mathrm{i} & 0 \end{pmatrix} + \omega E \in \mathbf{H}^0 \cap \mathbf{H}_1,$$

$$(2.8)\quad P^2 = \begin{pmatrix} -\omega & \overline{\omega} \\ -\omega & -\overline{\omega} \end{pmatrix} = \begin{pmatrix} -(1+\mathrm{i})/2 & (1-\mathrm{i})/2 \\ -(1+\mathrm{i})/2 & -(1-\mathrm{i})/2 \end{pmatrix} = -\begin{pmatrix} 1+\mathrm{i} & \mathrm{i} \\ 1+\mathrm{i} & 1 \end{pmatrix} + \omega E \in \mathbf{H}^1 \cap \mathbf{H}_0,$$

$$(2.9)\quad P^3 = -I,$$

$$(2.10)\quad Q := \begin{pmatrix} 0 & -(1-\mathrm{i})/\sqrt{2} \\ (1+\mathrm{i})/\sqrt{2} & 0 \end{pmatrix} = \rho \begin{pmatrix} 0 & \mathrm{i} \\ 1 & 0 \end{pmatrix} \in \mathbf{V},$$

$$(2.11)\quad Q^2 = -I.$$

Lemma 2.4 *With Q as in* (2.10) *we have*

$$(2.12)\qquad \mathbf{V} = \mathbf{G}Q = Q\mathbf{G},$$

$$(2.13)\qquad \mathbf{W}^0 = \mathbf{H}^0 Q = Q\mathbf{H}^0,$$

$$(2.14)\qquad \mathbf{W}^1 = \mathbf{H}^1 Q = Q\mathbf{H}^1,$$

$$(2.15)\qquad \mathbf{W}_0 = \mathbf{H}_0 Q = Q\mathbf{H}_0,$$

$$(2.16)\qquad \mathbf{W}_1 = \mathbf{H}_1 Q = Q\mathbf{H}_1,$$

$$(2.17)\qquad \mathbf{W} = \mathbf{H}Q = Q\mathbf{H}.$$

Proof Multiplication with Q/ρ transposes the rows or the columns among each other and multiplies each entry by i or 1, and so does not change the parity of the row and column sums; further $\det Q = 1$. This implies (2.12), and together with

$$\omega E Q = \rho\left(\begin{pmatrix} 0 & -1 \\ 0 & -1 \end{pmatrix} + \omega E\right) \quad \text{and} \quad Q\omega E = \rho\left(\begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix} + \omega E\right)$$

also (2.13)–(2.17). ■

Lemma 2.5 *With P as in* (2.7) *we have*

$$(2.18)\qquad (a)\quad \mathbf{H}^0 = \mathbf{G}P, \qquad (b)\quad \mathbf{W}^0 = \mathbf{G}QP = \mathbf{V}P,$$

$$(2.19)\qquad (a)\quad \mathbf{H}^1 = \mathbf{G}P^2, \qquad (b)\quad \mathbf{W}^1 = \mathbf{G}QP^2 = \mathbf{V}P^2,$$

$$(2.20)\qquad (a)\quad \mathbf{H}_0 = P^2\mathbf{G}, \qquad (b)\quad \mathbf{W}_0 = P^2Q\mathbf{G} = P^2\mathbf{V},$$

$$(2.21)\qquad (a)\quad \mathbf{H}_1 = P\mathbf{G}, \qquad (b)\quad \mathbf{W}_1 = PQ\mathbf{G} = P\mathbf{V}.$$

Proof (i) Let $A \in \mathbf{H}^0$ and $A = A' + \omega E$ with $A' \in \mathrm{M}(2, \mathbb{Z}[\mathrm{i}])$. Then

(2.22)

$$\begin{aligned} AP^2 &= \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \omega E\right)\left(\begin{pmatrix} -1-\mathrm{i} & -\mathrm{i} \\ -1-\mathrm{i} & -1 \end{pmatrix} + \omega E\right) \\ &= \begin{pmatrix} -(1+\mathrm{i})(a'+b') & -\mathrm{i}a' - b' \\ -(1+\mathrm{i})(c'+d') & -\mathrm{i}c' - d' \end{pmatrix} + \mathrm{i}E + \omega \begin{pmatrix} -2-2\mathrm{i}+a'+b' & -\mathrm{i}-1+a'+b' \\ -2-2\mathrm{i}+c'+d' & -\mathrm{i}-1+c'+d' \end{pmatrix} \end{aligned}$$

By Theorem 2.1 and since $\mathbf{S}$ is a group, we have $AP^2 \in \mathbf{G} \cup \mathbf{H}$. Since $a' + b'$ and $c' + d'$ are even by hypothesis, the entries of the last matrix in (2.22) are all even, so their products with ω are in $\mathbb{Z}[\mathrm{i}]$, therefore $AP^2 \in \mathbf{G}$. With (2.9) and $\mathbf{G} = -\mathbf{G}$, it follows that $A \in \mathbf{G}P$.

Conversely, if $A \in \mathbf{G}P$, then there is $A_1 \in \mathbf{G}$ such that

$$A = A_1 P = \begin{pmatrix} -\mathrm{i}a_1 - (1+\mathrm{i})b_1 & -\mathrm{i}a_1 \\ -\mathrm{i}c_1 - (1+\mathrm{i})d_1 & -\mathrm{i}c_1 \end{pmatrix} + \omega \begin{pmatrix} a_1 + b_1 - 1 & a_1 + b_1 - 1 \\ c_1 + d_1 - 1 & c_1 + d_1 - 1 \end{pmatrix} + \omega E,$$

so $A \in \mathbf{H}$ by (2.4), and the row sums of A are even.

This proves (2.18) (a); (2.18) (b) follows from (2.12) and $\mathbf{V}P = Q\mathbf{G}P = Q\mathbf{H}^0 = \mathbf{W}^0$.

(ii) Let $A \in \mathbf{H}^1$ and $A = A' + \omega E$ with $A' \in \mathrm{M}(2, \mathbb{Z}[\mathrm{i}])$. Then

$$(2.23)\; AP = \left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} + \omega E \right) \left(\begin{pmatrix} -\mathrm{i} & -\mathrm{i} \\ -(1+\mathrm{i}) & 0 \end{pmatrix} + \omega E \right)$$
$$= \begin{pmatrix} -\mathrm{i}a' - (1+\mathrm{i})b' & -\mathrm{i}a' \\ -\mathrm{i}c' - (1+\mathrm{i})d' & -\mathrm{i}c' \end{pmatrix} + \mathrm{i}E + \omega \begin{pmatrix} -1 - 2\mathrm{i} + a' + b' & -\mathrm{i} + a' + b' \\ -1 - 2\mathrm{i} + c' + d' & -\mathrm{i} + c' + d' \end{pmatrix}$$

By Theorem 2.1 and since $\mathbf{S}$ is a group, we have $AP \in \mathbf{G} \cup \mathbf{H}$. Since $a' + b'$ and $c' + d'$ are odd by hypothesis, the entries of the last matrix in (2.23) are all even in $\mathbb{Z}[\mathrm{i}]$, so that their products with ω are in $\mathbb{Z}[\mathrm{i}]$, therefore $AP \in \mathbf{G}$. With (2.9) and $\mathbf{G} = -\mathbf{G}$, it follows that $A \in \mathbf{G}P^2$.

Conversely, if $A \in \mathbf{G}P^2$, then there is $A_1 \in \mathbf{G}$ such that

$$A = A_1 P^2 = \begin{pmatrix} -(1+\mathrm{i})(a_1 + b_1) & -\mathrm{i}a_1 - b_1 \\ -(1+\mathrm{i})(c_1 + d_1) & -\mathrm{i}c_1 - d_1 \end{pmatrix} + \omega \begin{pmatrix} a_1 + b_1 - 1 & a_1 + b_1 - 1 \\ c_1 + d_1 - 1 & c_1 + d_1 - 1 \end{pmatrix} + \omega E,$$

so $A \in \mathbf{H}$ by (2.4), and the row sums of A are odd, again because of (2.4).

This proves (2.19) (a); (2.19) (b) follows from (2.12) and $\mathbf{V}P^2 = Q\mathbf{G}P^2 = Q\mathbf{H}^1 = \mathbf{W}^1$.

(iii) From (2.18) (a) and (2.19) (a), one obtains with (2.6) and (2.9)

$$\mathbf{H}_0 = (\mathbf{H}^0)^{-1} = P^{-1}\mathbf{G}^{-1} = -P^2\mathbf{G} = P^2\mathbf{G},$$
$$\mathbf{H}_1 = (\mathbf{H}^1)^{-1} = P^{-2}\mathbf{G}^{-1} = -P\mathbf{G} = P\mathbf{G},$$

which proves (2.20) (a) and (2.21) (a); (2.20) (b) and (2.21) (b) are proved analogously. ∎

3 Group Structure

Now we study the structure of the sets defined in Theorem 2.1.

Theorem 3.1 *$\mathbf{G}$ is a group. The only subgroups between $\mathbf{G}$ and $\mathbf{S}$ are $\mathbf{G} \cup \mathbf{H}$ and $\mathbf{G} \cup \mathbf{V}$. Furthermore*

(i) $[\mathbf{S} : \mathbf{G} \cup \mathbf{H}] = 2$ *with coset* $\mathbf{V} \cup \mathbf{W}$.

(ii) $[\mathbf{G} \cup \mathbf{H} : \mathbf{G}] = 3$ *with right cosets* $\mathbf{H}^0$ *and* $\mathbf{H}^1$ *and left cosets* $\mathbf{H}_0$ *and* $\mathbf{H}_1$.

(iii) $[\mathbf{S} : \mathbf{G} \cup \mathbf{V}] = 3$ *with right cosets* $\mathbf{H}^0 \cup \mathbf{W}^0$ *and* $\mathbf{H}^1 \cup \mathbf{W}^1$ *and left cosets* $\mathbf{H}_0 \cup \mathbf{W}_0$ *and* $\mathbf{H}_1 \cup \mathbf{W}_1$.

(iv) $[\mathbf{G} \cup \mathbf{V} : \mathbf{G}] = 2$ *with coset* $\mathbf{V}$.
(v) $[\mathbf{S} : \mathbf{G}] = 6$ *with right cosets* $\mathbf{H}^0$, $\mathbf{H}^1$, $\mathbf{V}$, $\mathbf{W}^0$, $\mathbf{W}^1$ *and left cosets* $\mathbf{H}_0$, $\mathbf{H}_1$, $\mathbf{V}$, $\mathbf{W}_0$, $\mathbf{W}_1$.

To each of the cosets in (i)–(v) a representative can be read off from the formulas in Lemmas 2.4 and 2.5. Subgroups of index 2 are always normal, hence their right and left cosets coincide. A further simple property of cosets is stated beforehand for the sake of reference.

Lemma 3.2 *If* $\mathbf{G}$, $\mathbf{G}'$, $\mathbf{S}$ *are groups and* $\mathbf{G} \subset \mathbf{G}' \subset \mathbf{S}$, *then a coset of* $\mathbf{G}$ *in* $\mathbf{S}$ *is either contained in* $\mathbf{G}'$ *or contained in* $\mathbf{S} \smallsetminus \mathbf{G}'$.

Proof of Theorem 3.1 The assertion is broken up in pieces which are dealt with one by one.

(A) $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, *and* $\mathbf{G} \cup \mathbf{V}$ *are subgroups of* $\mathbf{S}$. It follows from (2.2) that $A \mapsto A^{-1}$ maps each of $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, and $\mathbf{G} \cup \mathbf{V}$ onto itself. Therefore it remains to show that a product A_1A_2 of matrices in $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, or $\mathbf{G} \cup \mathbf{V}$ is again an element of $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, or $\mathbf{G} \cup \mathbf{V}$, respectively.

If $A_1, A_2 \in \mathbf{G}$, then the sum of the components of A_1A_2 is

$$a_1a_2 + b_1c_2 + a_1b_2 + b_1d_2 + c_1a_2 + d_1c_2 + c_1b_2 + d_1d_2 \\ = (a_1 + c_1)(a_2 + b_2) + (b_1 + d_1)(c_2 + d_2),$$

which is even according to (2.4), so $A_1A_2 \in \mathbf{G}$ by (2.3).

If $A_1, A_2 \in \mathbf{G} \cup \mathbf{H}$, then $A_1A_2 \notin \mathbf{V}$ and $A_1A_2 \notin \mathbf{W}$. Hence $A_1A_2 \in \mathbf{G} \cup \mathbf{H}$ by Theorem 2.1.

If $A_1A_2 \in \mathbf{G} \cup \mathbf{V}$, then $A_1A_2 \notin \mathbf{H}$ and $A_1A_2 \notin \mathbf{W}$. Hence $A_1A_2 \in \mathbf{G} \cup \mathbf{V}$ by Theorem 2.1.

(B) *The right and left cosets of* $\mathbf{G}$ *in* $\mathbf{S}$ *are* $\mathbf{H}^0, \mathbf{H}^1, \mathbf{V}, \mathbf{W}^0, \mathbf{W}^1$ *and* $\mathbf{H}_0, \mathbf{H}_1, \mathbf{V}, \mathbf{W}_0, \mathbf{W}_1$, *respectively.* It follows from Theorem 2.1 and (2.5) that $\mathbf{S}$ is the union of the pairwise disjoint sets $\mathbf{G}$, $\mathbf{H}^0$, $\mathbf{H}^1$, $\mathbf{V}$, $\mathbf{W}^0$, $\mathbf{W}^1$. By (2.18), (2.19), and (2.12) they satisfy $\mathbf{H}^0 = \mathbf{G}P$, $\mathbf{H}^1 = \mathbf{G}P^2$, $\mathbf{V} = \mathbf{G}Q$, $\mathbf{W}^0 = \mathbf{G}QP$, $\mathbf{W}^1 = \mathbf{G}QP^2$. Since $\mathbf{G}$ is a group, these 5 sets are the right cosets of $\mathbf{G}$ in $\mathbf{S}$. Similarly, $\mathbf{H}_0 = P^2\mathbf{G}$, $\mathbf{H}_1 = P\mathbf{G}$, $\mathbf{V} = Q\mathbf{G}$, $\mathbf{W}_0 = P^2Q\mathbf{G}$, $\mathbf{W}_1 = PQ\mathbf{G}$ are the left cosets of $\mathbf{G}$ in $\mathbf{S}$.

(C) $\mathbf{V} \cup \mathbf{W}$ *is the coset of the subgroup* $\mathbf{G} \cup \mathbf{H}$ *in* $\mathbf{S}$. This follows from Theorem 2.1, (2.12), and (2.17). It implies that there are no other subgroups containing $\mathbf{G} \cup \mathbf{H}$.

(D) *If* $\mathbf{G}'$ *is a group and* $\mathbf{G} \subset \mathbf{G}' \subset \mathbf{S}$, *then both* $\mathbf{H}$ *and* $\mathbf{V}$ *are either contained in* $\mathbf{G}'$ *or in* $\mathbf{S} \smallsetminus \mathbf{G}'$. The alternatives $\mathbf{V} \subset \mathbf{G}'$ or $\mathbf{V} \subset \mathbf{S} \smallsetminus \mathbf{G}'$, $\mathbf{H}^0 \subset \mathbf{G}'$ or $\mathbf{H}^0 \subset \mathbf{S} \smallsetminus \mathbf{G}'$, and $\mathbf{H}^1 \subset \mathbf{G}'$ or $\mathbf{H}^1 \subset \mathbf{S} \smallsetminus \mathbf{G}'$ follow directly from (B) and Lemma 3.2. First of all, this proves the assertion for $\mathbf{V}$.

If $\mathbf{H}^0 \subset \mathbf{G}'$, then $P \in \mathbf{G}'$ by (2.7). Hence $\mathbf{H}^1 = \mathbf{G}P^2 \subset \mathbf{G}'$ by (2.19) (a); similarly, if $\mathbf{H}^1 \subset \mathbf{G}'$, then $P^2 \in \mathbf{G}'$ by (2.8), Hence $\mathbf{H}^0 = \mathbf{G}P = -\mathbf{G}P^2P^2 \subset \mathbf{G}'$ by (2.9) and (2.18) (a). Hence the assertion is true also for $\mathbf{H}$.

(E) *If* $\mathbf{G}'$ *is a group and* $\mathbf{G} \subset \mathbf{G}' \subset \mathbf{S}$, *then* $\mathbf{G}' = \mathbf{S}$ *or* $\mathbf{W} \subset \mathbf{S} \smallsetminus \mathbf{G}'$. If $\mathbf{W} \cap \mathbf{G}' \neq \varnothing$, then $\mathbf{W}^0 \subset \mathbf{G}'$ or $\mathbf{W}^1 \subset \mathbf{G}'$ by (B) and Lemma 3.2. If $\mathbf{W}^0 \subset \mathbf{G}'$, then it follows from (2.13) that $\mathbf{G}' \supset (\mathbf{W}^0)^2 = \mathbf{H}^0QQ\mathbf{H}^0 = -(\mathbf{H}^0)^2$. Hence $P^{-1} = -P^2 \in \mathbf{G}'$ by (2.7), Hence $P \in \mathbf{G}'$. Therefore $\mathbf{H}^0 = \mathbf{G}P \subset \mathbf{G}'$ by (2.18). If $\mathbf{W}^1 \subset \mathbf{G}'$, then it follows from (2.14)

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

that $\mathbf{G}' \supset (\mathbf{W}^1)^2 = \mathbf{H}^1 QQ\mathbf{H}^1 = -(\mathbf{H}^1)^2$. Hence $-P^4 \in \mathbf{G}'$ by (2.8). Hence $P \in \mathbf{G}'$ by (2.9) Therefore $\mathbf{H}^1 = \mathbf{G}P^2 \subset \mathbf{G}'$ by (2.19). Because of (D), it follows in both cases that $\mathbf{H} \subset \mathbf{G}'$. Hence $\mathbf{G} \cup \mathbf{H} \subset \mathbf{G}'$. But then (C) and $\mathbf{W} \cap \mathbf{G}' \neq \varnothing$ imply that $\mathbf{G}' = \mathbf{S}$.

(F) $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, *and* $\mathbf{G} \cup \mathbf{V}$ *are the only subgroups of* $\mathbf{S}$ *containing* $\mathbf{G}$. By (D) and (E) the sets $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, $\mathbf{G} \cup \mathbf{V}$, and $\mathbf{G} \cup \mathbf{H} \cup \mathbf{V}$ are the only candidates. The first three are indeed subgroups by (A), and the last drops out because of (C).

(G) It remains to prove (ii), (iii), and (iv).

(ii) This follows from Lemma 2.5 (a) and (2.5).

(iii) From (2.18) and (2.19) it follows that $(\mathbf{G} \cup \mathbf{V})P = \mathbf{H}^0 + \mathbf{W}^0$ and $(\mathbf{G} \cup \mathbf{V})P^2 = \mathbf{H}^1 + \mathbf{W}^1$. From Theorem 2.1 and (2.5) it now follows that $\mathbf{H}^0 + \mathbf{W}^0$ and $\mathbf{H}^1 + \mathbf{W}^1$ are the right cosets of $\mathbf{G} \cup \mathbf{V}$ in $\mathbf{S}$. Similarly, $\mathbf{H}_0 + \mathbf{W}_0$ and $\mathbf{H}_1 + \mathbf{W}_1$ are the left cosets.

(iv) This follows from (2.12). ∎

While subgroups of index 2 are always normal, the subgroups in (ii), (iii), and (v) are not.

Corollary 3.3 $\mathbf{G}$ *is neither normal in* $\mathbf{G} \cup \mathbf{H}$ *nor in* $\mathbf{S}$*;* $\mathbf{G} \cup \mathbf{V}$ *is not normal in* $\mathbf{S}$.

Proof If $\mathbf{G}$ were normal in $\mathbf{G} \cup \mathbf{H}$, then $A\mathbf{G} = \mathbf{G}A$ for every $A \in \mathbf{G} \cup \mathbf{H}$; moreover, because of (2.12), we would have $QA\mathbf{G} = Q\mathbf{G}A = \mathbf{G}QA$ for every $A \in \mathbf{G} \cup \mathbf{H}$. Since every element of $\mathbf{S}$ belongs to $\mathbf{G} \cup \mathbf{H}$ or $Q(\mathbf{G} \cup \mathbf{H})$, this shows that $\mathbf{G}$ were normal in $\mathbf{S}$.

If $\mathbf{G} \cup \mathbf{V}$ were normal in $\mathbf{S}$, then $A(\mathbf{G} \cup \mathbf{V}) = (\mathbf{G} \cup \mathbf{V})A$. Hence

$$A\mathbf{G} \cup A\mathbf{V} = \mathbf{G}A \cup \mathbf{V}A$$

for all $A \in \mathbf{S}$. We sort the matrices on both sides according to their number of ρ-factors. If $A \in (\mathbf{G} \cup \mathbf{H})$, then the matrices without a ρ-factor are those in $A\mathbf{G}$ and $\mathbf{G}A$, hence $A\mathbf{G} = \mathbf{G}A$. If $A \in (\mathbf{V} \cup \mathbf{W})$, then the matrices with exactly one ρ-factor are those in $A\mathbf{G}$ and $\mathbf{G}A$, so $A\mathbf{G} = \mathbf{G}A$ again. Since $A\mathbf{G} = \mathbf{G}A$ for all $A \in \mathbf{S}$, the subgroup $\mathbf{G}$ was normal in $\mathbf{S}$.

Therefore it is sufficient to show that $\mathbf{G}$ is not normal in $\mathbf{S}$. We assume the contrary. Then $\mathbf{S}/\mathbf{G}$ can be represented by the system of cosets of $\mathbf{G}$, with the multiplication of complexes as binary operation. By (2.13) and (2.14) we have $\mathbf{W}^0 = \mathbf{G}PQ$ and $\mathbf{W}^1 = \mathbf{G}P^2Q$. Since by reason of our assumption $\mathbf{G}$ commutes with every element of $\mathbf{S}$, we obtain

$$(\mathbf{W}^0)^2 = \mathbf{G}(PQ)^2 = \mathbf{G}\begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} = \mathbf{G} \quad \text{and} \quad (\mathbf{W}^1)^2 = \mathbf{G}(P^2Q)^2 = \mathbf{G}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \mathbf{G},$$

Therefore $\mathbf{W}^0 = \mathbf{G}PQ$ and $\mathbf{W}^1 = \mathbf{G}P^2Q$ have order 2 in $\mathbf{S}/\mathbf{G}$. Hence $(\mathbf{W}^0)^{-1} = \mathbf{W}^0$ and $(\mathbf{W}^1)^{-1} = \mathbf{W}^1$. From (2.13) and (2.14), it now follows that $(\mathbf{H}^0)^{-1} = \mathbf{H}^0$ and $(\mathbf{H}^1)^{-1} = \mathbf{H}^1$. Therefore by (2.6), $\mathbf{H}_0 = \mathbf{H}^0$ and $\mathbf{H}_1 = \mathbf{H}^1$. This implies that the parity of the column sums matches that of the row sums for all elements of $\mathbf{H}$, which, for instance, is wrong for P and P^2. ∎

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

4 Generators of S and Its Subgroups

We establish for each of the groups $\mathbf{G}$, $\mathbf{G} \cup \mathbf{H}$, $\mathbf{G} \cup \mathbf{V}$, and $\mathbf{S}$ finite sets $\{A_1, A_2, \dots\}$ of generators such that all elements of the group are products of positive powers of the generators. The group is then written $\langle A_1, A_2, \dots \rangle$.

For this purpose we apply a reduction procedure advised by H. S. M. Coxeter [8, Appendix] and used in [5, §2]; the most important step is the introduction of the transformations C_1 and C_2 in (4.6) below. The method does not deal directly with the matrices $A \in \mathbf{S}$, but rather with their four-dimensional counterparts L_A in (1.2); Unlike Coxeter and Lorente–Kramer, we avoid spatial reflections.

4.1 Spatial Rotations

The Lorentz transformations of the form $L_A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & D_A \end{smallmatrix}\right)$ correspond to the rotations of $\mathbb{R}^3$. Then $D_A \in \mathrm{SO}(3)$, and the L_A of this kind build a subgroup $1 \oplus \mathrm{SO}(3)$ of $\mathrm{SO}^+(1,3)$. We consider the group

$$\mathbf{R} := \mathbf{S} \cap \{A : L_A \in 1 \oplus \mathrm{SO}(3)\} = \{A : D_A \in \mathrm{SO}(3) \cap \mathrm{M}(3, \mathbb{Z})\}.$$

Clearly $A \mapsto D_A$ is a group homomorphism of $\mathbf{R}$ into $\mathrm{SO}(3) \cap \mathrm{M}(3, \mathbb{Z})$.

We show first that $P \in \mathbf{H}$ and $Q \in \mathbf{V}$, defined in (2.7) and (2.10), belong to $\mathbf{R}$. From

$$P \begin{pmatrix} t+z & x+\mathrm{i}y \\ x-\mathrm{i}y & t-z \end{pmatrix} P^* \begin{pmatrix} t+x & y+\mathrm{i}z \\ y-\mathrm{i}z & t-x \end{pmatrix}$$

and (1.7), it follows that $L_P \in 1 \oplus \mathrm{SO}(3)$ and

$$D_P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Hence $P \in \mathbf{R}$, and D_P causes a rotation through 120° about $\{(x, y, z) : x = y = z\}$. Furthermore,

$$Q \begin{pmatrix} t+z & x+\mathrm{i}y \\ x-\mathrm{i}y & t-z \end{pmatrix} Q^* = \begin{pmatrix} t-z & y+\mathrm{i}x \\ y-\mathrm{i}x & t+z \end{pmatrix},$$

so (1.7) shows that $L_Q \in 1 \oplus \mathrm{SO}(3)$ and

$$D_Q = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Hence $Q \in \mathbf{R}$, and L_Q causes a rotation through 180° about $\{(x, y, z) : x = y,\ z = 0\}$.

Lemma 4.1 $\mathbf{R} = \langle P, Q \rangle$.

Proof Because of the orthogonality, each row and column of a matrix $D \in \mathrm{SO}(3) \cap \mathrm{M}(3, \mathbb{Z})$ contains two 0's and one entry from $\{-1, 1\}$. Hence D is a permutation matrix if the signs are ignored. By virtue of $\det D = 1$ the number of minus signs is even, if the permutation is even, and odd otherwise. So all elements of $\mathrm{SO}(3) \cap \mathrm{M}(3, \mathbb{Z})$ are obtained from the six permutation matrices and the allocation of none or two minus signs in the matrices of the even and one or three minus signs in those of the odd

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

permutations. It follows that $\mathrm{SO}(3)\cap \mathrm{M}(3,\mathbb{Z})$ has 24 elements and is the same as the *cube* or *octahedral group*. On the other hand, if the 8 matrices

$$D_I=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad D_{QP^2QP}=\begin{pmatrix}0&0&1\\-1&0&0\\0&-1&0\end{pmatrix},\quad D_{QPQP^2}=\begin{pmatrix}0&-1&0\\0&0&1\\-1&0&0\end{pmatrix},\tag{4.1}$$
$$D_{P^2QPQ}=\begin{pmatrix}0&-1&0\\0&0&1\\-1&0&0\end{pmatrix},\quad D_Q=\begin{pmatrix}0&1&0\\1&0&0\\0&0&-1\end{pmatrix},\quad D_{P^2QP}=\begin{pmatrix}-1&0&0\\0&0&1\\0&1&0\end{pmatrix},$$
$$D_{PQP^2}=\begin{pmatrix}0&0&1\\0&-1&0\\1&0&0\end{pmatrix},\quad D_{QP^2QPQ}=\begin{pmatrix}0&0&-1\\0&-1&0\\-1&0&0\end{pmatrix}$$

are multiplied from the right with D_I, D_P and D_{P^2}, we obtain 24 different matrices. Therefore D_P and D_Q generate $\mathrm{SO}(3)\cap\mathrm{M}(3,\mathbb{Z})$. ∎

Lemma 4.2 $\mathbf{R}\cap\mathbf{G}=\langle B_1,B_2\rangle$.

Proof Let $A\in\mathbf{R}\cap\mathbf{G}$. Since $L_A\in 1\oplus\mathrm{SO}(3)$, it follows from (1.3) that $|a|^2+|b|^2+|c|^2+|d|^2=2$. Since $a,b,c,d\in\mathbb{Z}[\mathrm{i}]$, the components of one diagonal of A are units of $\mathbb{Z}[\mathrm{i}]$ and therefore have the form i^k and i^l ($k,l\in\{0,1,2,3,\}$), and the components of the other diagonal are 0. If the non-zero elements are in the main diagonal, then the condition $1=\det A=\mathrm{i}^{k+l}$ gives $k=l=0$ or $k=1$, $l=3$ or $k=l=2$, or $k=3$, $l=1$. The corresponding matrices are $\pm B_0$ and $\pm B_1$, where

$$B_0:=I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad B_1:=\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix}.$$

If the non-zero elements are in the secondary diagonal, then $1=\det A=-\mathrm{i}^{k+l}$ gives $k=0$, $l=2$ or $k=1$, $l=1$ or $k=2$, $l=0$, or $k=3$, $l=3$. The corresponding matrices are $\pm B_2$ and $\pm B_3$, where

$$B_2:=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad B_3:=\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix}.$$

The matrices $Z_j:=L_{B_j}$ ($j=0,1,2,3$) are

$$Z_0=I,\quad Z_1=\mathrm{diag}(1,-1,-1,1),\quad Z_2=\mathrm{diag}(1,-1,1,-1),\quad Z_3=\mathrm{diag}(1,1,-1,-1).\tag{4.2}$$

Therefore $B_j\in\mathbf{R}$ for $j=0,1,2,3$. Hence $\mathbf{R}\cap\mathbf{G}=\{\pm B_0,\pm B_1,\pm B_2,\pm B_3,\}$. Now the assertion follows from $B_3=B_1^3B_2$. Since $B_j^2=-I$ for $j=1,2,3$, the group $\mathbf{R}\cap\mathbf{G}$ is not cyclic, so at least two generators are necessary. ∎

Lemma 4.3 $\mathbf{R}\cap(\mathbf{G}\cup\mathbf{H})=\langle P,B_2\rangle$.

Proof We refer to the proof of Lemma 4.1 and consider the two possibilities for the elements of $\mathbf{R}$. The products of D_I, D_P, D_{P^2} with the last four matrices in (4.1) have the form D_A where A is a product of P-factors and an odd number of Q-factors. Hence the entries of A are rational multiples of ρ, so A cannot belong to $\mathbf{G}\cup\mathbf{H}$. Each of the products of D_I, D_P, D_{P^2} with the first four matrices in (4.1) has none or two entries equal to -1. They produce Lorentz transformations in $1 \oplus \mathrm{SO}(3)$ which arise from even 3×3 permutation matrices through the allocation of none or two minus signs; therefore they have representations as products of D_P- and Z_2-factors. Hence they have the form L_A with $A \in \mathbf{G} \cup \mathbf{H}$. ■

4.2 The Reduction Procedure

After these preparations we can construct generators for the groups considered in Theorem 3.1.

Theorem 4.4 *The group* **G** *is generated by*

$$(4.3)\quad V := \begin{pmatrix} 1 & 1+\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad \overline{V} := \begin{pmatrix} 1 & 1-\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

i.e.,

$$(4.4)\qquad \mathbf{G} = \langle V, \overline{V}, B_1, B_2 \rangle.$$

Proof The matrices V and $\overline{V}$ belong to **G** and

$$(4.5)\qquad L_V = \begin{pmatrix} 2 & 1 & 1 & -1 \\ 1 & 1 & 0 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad L_{\overline{V}} = \begin{pmatrix} 2 & 1 & -1 & -1 \\ 1 & 1 & 0 & -1 \\ -1 & 0 & 1 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}.$$

Let

$$(4.6)\qquad C_1 := L_V Z_1 = L_{VB_1} = \begin{pmatrix} 2 & -1 & -1 & -1 \\ 1 & -1 & 0 & -1 \\ 1 & 0 & -1 & -1 \\ 1 & -1 & -1 & 0 \end{pmatrix},$$

$$C_2 := L_{\overline{V}} Z_3 = L_{\overline{V}B_3} = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ -1 & 0 & -1 & -1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

For $A \in \mathbf{G}$ we write

$$L_A = \begin{pmatrix} \alpha & \epsilon & \zeta & \eta \\ \beta & * & * & * \\ \gamma & * & * & * \\ \delta & * & * & * \end{pmatrix}.$$

Then

$$(4.7)\qquad \alpha^2 - \beta^2 - \gamma^2 - \delta^2 = \alpha^2 - \epsilon^2 - \zeta^2 - \eta^2 = 1.$$

It is seen from (1.3) that $\alpha > 0$. If $\alpha = 1$, then $L_A \in 1 \oplus \mathrm{SO}(3)$ and $A \in \mathbf{R}$. Now let $\alpha > 1$.

We multiply L_A from the left with a suitable matrix Z_k from (4.2) such that the second, third, and fourth elements in the first column of $Z_k L_A$ have the same sign

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

and obtain

$$(4.8)\qquad Z_k L_A = L_{B_k A} = \begin{pmatrix} \alpha & \epsilon & \zeta & \eta \\ \beta' & * & * & * \\ \gamma' & * & * & * \\ \delta' & * & * & * \end{pmatrix},$$

where

(i) $\beta' \geq 0, \gamma' \geq 0, \delta' \geq 0$ or
(ii) $\beta' \leq 0, \gamma' \leq 0, \delta' \leq 0$.

In case (i), we consider

$$(4.9)\qquad C_1 L_{B_k A} = L_{V B_1 B_k A} = \begin{pmatrix} 2\alpha - \beta' - \gamma' - \delta' & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix},$$

and in case (ii)

$$(4.10)\qquad C_2 L_{B_k A} = L_{\overline{V} B_3 B_k A} = \begin{pmatrix} 2\alpha + \beta' + \gamma' + \delta' & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}.$$

Because of (4.7) we have $\alpha^2 - \beta'^2 - \gamma'^2 - \delta'^2 = \alpha^2 - \beta^2 - \gamma^2 - \delta^2 = 1$. Therefore in (4.9) and (4.10) at least two of the numbers α', β', γ' are different from 0, so in both cases at least one of the products $\alpha'\beta', \beta'\gamma', \gamma'\alpha'$ is positive. It follows that

$$(\alpha + \beta' + \gamma' + \delta')(\alpha - \beta' - \gamma' - \delta') = 1 - 2\alpha'\beta' - 2\beta'\gamma' - 2\gamma'\alpha' < 0.$$

Therefore $\alpha - \beta' - \gamma' - \delta' < 0$ and $2\alpha - \beta' - \gamma' - \delta' < \alpha$ in case (i), and $\alpha + \beta' + \gamma' + \delta' < 0$ and $2\alpha + \beta' + \gamma' + \delta' < \alpha$ in case (ii).

In both cases a product S_1 of factors from $\{B_1, B_2, B_3, V, \overline{V}\} \subset \mathbf{G}$ was found such that the element in the first row and column of $L_{S_1 A}$ is smaller than that of L_A. Continuing in this way we construct $L_{S_2 S_1 A}, L_{S_3 S_2 S_1 A}$, etc., until after n steps this element is reduced to 1. If $A \in \mathbf{G}$, then $L_{S_n \cdots S_1 A} \in \mathbf{R}$ and $S_n \cdots S_1 A \in \mathbf{G}$. Hence $S_n \cdots S_1 A \in 1 \oplus \mathrm{SO}(3)$, $A \in S_1^{-1} \cdots S_n^{-1}(1 \oplus \mathrm{SO}(3))$, so by Lemma 4.2 and the structure of the S_ν, A is a product of factors of the form B_1, B_2, B_1^{-1}, B_2^{-1}, B_3^{-1}, V^{-1}, $\overline{V}^{-1}$. By means of $B_1^{-1} = B_1^3$, $B_2^{-1} = B_1^2 B_2$, $B_3^{-1} = B_1 B_2$, $V^{-1} = B_1^3 V B_1$, $\overline{V}^{-1} = B_1^3 \overline{V} B_1$, and $-I = B_1^2$ we can eliminate the inverses and possible negative signs and replace them with products of positive powers of B_1, B_2, V, and $\overline{V}$. This proves (4.4). ■

Theorem 4.5 *The group* $\mathbf{G} \cup \mathbf{H}$ *is generated by*

$$V = \begin{pmatrix} 1 & 1+\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad \overline{V} = \begin{pmatrix} 1 & 1-\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad B_2 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$P = \begin{pmatrix} (1-\mathrm{i})/2 & (1-\mathrm{i})/2 \\ -(1+\mathrm{i})/2 & (1+\mathrm{i})/2 \end{pmatrix},$$

i.e.,

$$(4.11)\qquad \mathbf{G} \cup \mathbf{H} = \langle V, \overline{V}, B_2, P \rangle.$$

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

Proof Let $A \in \mathbf{G} \cup \mathbf{H}$. We must apply the reduction procedure once more. The proof is the same as for Theorem 4.4, except that we admit L_P as an additional multiplier in the step leading to (4.8). Due to $B_1, B_3 \in \langle P, B_2 \rangle$, according to Lemma 4.3, besides L_P only Z_2 is necessary to reach (i) or (ii).

The multipliers S_ν belong to $\langle V, \overline{V}, B_2, P \rangle$. In the final step of the recursion we arrive at $L_{S_n \cdots S_1 A} \in \mathbf{R}$ and $S_n \cdots S_1 A \in \mathbf{G} \cup \mathbf{H}$. By Lemma 4.3, $S_n \cdots S_1 A \in \langle P, B_2 \rangle$. Hence $A \in S_1^{-1} \cdots S_n^{-1} \langle P, B_2 \rangle$, so A is a product of factors B_1, B_1^{-1}, P, P^2, V^{-1}, and $\overline{V}^{-1}$. By means of $B_1^{-1} = B_1^3$, $V^{-1} = B_1^3 V B_1$, $\overline{V}^{-1} = B_1^3 \overline{V} B_1$, $-I = B_1^2$, and $B_1 = P B_2 P^{-1}$ we eliminate the inverses and negative signs and replace them with products of positive powers of B_2, V, $\overline{V}$, and P. This proves (4.11). ■

Theorem 4.6 *The group* $\mathbf{G} \cup \mathbf{V}$ *is generated by*

$$V = \begin{pmatrix} 1 & 1+\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad \overline{V} = \begin{pmatrix} 1 & 1-\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad B_2 := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$Q = \begin{pmatrix} 0 & -(1-\mathrm{i})/\sqrt{2} \\ (1+\mathrm{i})/\sqrt{2} & 0 \end{pmatrix},$$

i.e., $\mathbf{G} \cup \mathbf{V} = \langle V, \overline{V}, B_2, Q \rangle$.

Proof This follows from (2.12), Theorem 4.4, and $B_1 = (B_2 Q)^2$. ■

Theorem 4.7 *The group* $\mathbf{S}$ *is generated by*

$$V = \begin{pmatrix} 1 & 1+\mathrm{i} \\ 0 & 1 \end{pmatrix}, \quad P = \begin{pmatrix} (1-\mathrm{i})/2 & (1-\mathrm{i})/2 \\ -(1+\mathrm{i})/2 & (1+\mathrm{i})/2 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & -(1-\mathrm{i})/\sqrt{2} \\ (1+\mathrm{i})/\sqrt{2} & 0 \end{pmatrix},$$

i.e., $\mathbf{S} = \langle V, P, Q \rangle$.

Remarks (1) Only three generators are sufficient, whereas four seem to be necessary if reflections are allowed (*cf.* the transformations S_1, S_2, S_3, S_4 in [5, §2]).

(2) While the generators P and Q are rotations which leave the time axis fixed, V incorporates a boost, as we show in the following section.

Proof of Theorem 4.7 Similarly to the proofs of Theorem 4.4 and 4.5, we must resort to the reduction procedure. This time we have the multipliers L_P and L_Q at our disposal for the step leading to (4.8). With them we can always reach case (i) in (4.8), so the matrix C_2 is not needed. The multipliers S_ν belong to $\langle V, P, Q \rangle$. In the final step we arrive at $L_{S_n \cdots S_1 A} \in 1 \oplus \mathrm{SO}(3)$. Hence $S_n \cdots S_1 A \in \mathbf{R}$. From Lemma 4.1 it follows that $A \in S_1^{-1} \cdots S_n^{-1} \langle P, Q \rangle$, so A is a product of factors P, P^2, Q, and $V^{-1} = B_1^3 V B_1$. Since $B_1 \in \mathbf{R} = \langle P, Q \rangle$, we can write A as a product of positive powers of P, Q, and V. ■

5 Decompositions in Boost and Rotation

A restricted Lorentz transformation can be decomposed into a boost and a subsequent rotation or the other way round, in each case in a unique manner [3, Chapter 7-2]. For a boost, the matrix A in (1.2) is Hermitian and for a rotation, it is unitary [7, §1.2]. To

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

deal with the general situation in other cases, it is convenient to refer to the kinematic representation of Lorentz transformations. If L_A is defined as in (1.7) and the 4×4 matrices are written in $(1,3)$-block form, then

(5.1)

$$L_A = L(\vec{v}, D) := \begin{pmatrix} 1 & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} \gamma & -\gamma\vec{v}^{\top} \\ -\gamma\vec{v} & I + (\gamma - 1)\dfrac{\vec{v}\,\vec{v}^{\top}}{v^2} \end{pmatrix} = \begin{pmatrix} \gamma & -\gamma\vec{v}^{\top} \\ -\gamma\vec{u} & D + (\gamma - 1)\dfrac{\vec{u}\,\vec{v}^{\top}}{v^2} \end{pmatrix},$$

where $\gamma = \frac{1}{\sqrt{1-v^2}}$. This is the concatenation of a boost and a spatial rotation. The 3-vector $\vec{v}$ is the velocity of the primed system with respect to the unprimed according to (1.7), and $v = \sqrt{|\vec{v}|^2}$. The 3×3 matrix D is orthogonal with $\det D = 1$. Furthermore, $\vec{u} = D\vec{v}$.

If the range of Lorentz transformations is confined to integral transformations, then the 24 matrices in $\mathbf{R}$ produce all possible rotations, so $\mathbf{R}$ is equal to the set of unitary matrices in $\mathbf{S}$. Furthermore, there is an infinite set of Hermitian matrices which produce boosts with integer components, *e.g.*, the matrices in $\mathbf{G}$, given by

$$A(p,q) = \begin{pmatrix} p^2 + q^2 + 1 & p + \mathrm{i}q \\ p - \mathrm{i}q & 1 \end{pmatrix}, \qquad p,\ q \in \mathbb{Z} \text{ both even or both odd.}$$

Nevertheless, in contrast to the situation for general restricted Lorentz transformations, it is not possible to write every matrix in $\mathbf{S}$ as the product of a Hermitian matrix and a unitary matrix. An example is L_V, displayed in (4.5), where V is defined in (4.3). We compare it with the kinematic form analogous to (5.1).

The ansatz $L_V = L(\vec{v}, D)$ leads to $\gamma = 2$. Hence $v = \frac{1}{2}\sqrt{3}$ and

$$L_V = \begin{pmatrix} 2 & -2\vec{v}^{\top} \\ -2\vec{u} & D + \frac{4}{3}\vec{u}\,\vec{v}^{\top} \end{pmatrix}.$$

Therefore $\vec{v}^{\top} = (-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2})$, $\vec{u}^{\top} = (-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2})$ and

$$D = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 1 & 1 & 0 \end{pmatrix} - \frac{1}{3}\begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 2/3 & -1/3 & -2/3 \\ -1/3 & 2/3 & -2/3 \\ 2/3 & 2/3 & 1/3 \end{pmatrix}.$$

Then D is orthogonal and $\det D = 1$, as expected; since $(1,-1,0)^{\top}$ is a fixed point of D, it causes a rotation about the axis $\{(x,y,z) : y = -x,\ z = 0\}$. The decomposition in (5.1) is

$$L_V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2/3 & -1/3 & -2/3 \\ 0 & -1/3 & 2/3 & -2/3 \\ 0 & 2/3 & 2/3 & 1/3 \end{pmatrix} \begin{pmatrix} 2 & 1 & 1 & -1 \\ 1 & 4/3 & 1/3 & -1/3 \\ 1 & 1/3 & 4/3 & -1/3 \\ -1 & -1/3 & -1/3 & 4/3 \end{pmatrix}.$$

None of the factors is in $\mathbf{S}$, *i.e.*, the uniquely determined factors in the decomposition of L_V in boost and rotation are not matrices with integer components.

6 Relation to the Picard Group

The group $\mathbf{G}$ consists of those elements of $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$ which via $A \mapsto L_A$ generate integral Lorentz transformations; $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$ will be referred to as a *Picard group*. The

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

use of this term is not uniform; sometimes it stands for $\mathrm{PSL}(2,\mathbb{Z}[\mathrm{i}])$, for instance, in [2], where the subgroups of $\mathrm{PSL}(2,\mathbb{Z}[\mathrm{i}])$ are extensively studied. For our subject this distinction is inessential.

Let $A \in \mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$. From $1 = \det A \equiv \pi(a)\pi(d) - \pi(b)\pi(c)$ it follows that exactly three components of A are odd, or the members of one diagonal are odd and those of the other even. We call $A_1, A_2 \in \mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$ congruent if homologous components have the same parity (see subsection 1.1). Then A is congruent to exactly one of the six matrices

$$K_0 := I, \quad K_1 := \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad K_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad K_3 = K_1K_2 = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & \mathrm{i} \end{pmatrix},$$
$$K_4 := K_2K_1 = \begin{pmatrix} \mathrm{i} & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad K_5 := K_1\,K_2K_1 = -\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

This decomposes $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$ into six disjoint classes $\mathbf{K}_j$ $(j = 0,1,2,3,4,5)$ such that every $A \in \mathbf{K}_j$ has a representation

$$A = (1+\mathrm{i})A' + K_j \tag{6.1}$$

with $A' \in \mathrm{M}(2,\mathbb{Z}[\mathrm{i}])$ and uniquely determined $j \in \{0,1,2,3,4,5\}$.

Lemma 6.1 (see [2, Theorem 2 (3)]) $\mathbf{K}_0$ *is a normal subgroup of* $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$ *of index* 6 *with cosets* $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3, \mathbf{K}_4, \mathbf{K}_5$. *The factor group is the non-cyclic group of order* 6. *It has the cyclic subgroup* $\{\mathbf{K}_0, \mathbf{K}_3, \mathbf{K}_4\}$; *furthermore,* $\mathbf{K}_1^2 = \mathbf{K}_2^2 = \mathbf{K}_5^2 = \mathbf{K}_0$.

Proof It is evident that $\mathbf{K}_0$ is a subgroup of $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$. Since each of the expressions $K_0, -K_1^2, 2K_2 - K_2^2, \mathrm{i}K_3 - K_3^2, \mathrm{i}K_4 - K_4^2$, and $-2K_5 - K_5^2$ represents the identity matrix I, we can factor out K_j in (6.1) to the right or to the left and obtain $A \in \mathbf{K}_0K_j$ and $A \in K_j\mathbf{K}_0$. Since this holds for every $A \in \mathbf{K}_j$, it follows that $K_j\mathbf{K}_0 = \mathbf{K}_0K_j$, *i.e.*, for each j the right coset of $\mathbf{K}_0$ with respect to K_j coincides with the left coset with respect to K_j and is equal to $\mathbf{K}_j$. Therefore $\mathbf{K}_0$ is normal. The factor group $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])/\mathbf{K}_0$ can be represented by the system of cosets, with the multiplication of complexes as binary operation. ■

Theorem 6.2 $\mathbf{K}_0$ *is a subgroup of index* 2 *in* $\mathbf{G}$; $\mathbf{G}$ *is a subgroup of index* 3 *in*

$$\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}]),$$

but not a normal subgroup.

Proof If $A \in \mathbf{G}$, then $\|A\|^2$ must be even. Hence $\pi(a)+\pi(b)+\pi(c)+\pi(d) = 0$. This is impossible with three odd components, so $j = 0$ or $j = 1$ in (6.1) and $\mathbf{G} = \mathbf{K}_0 \cup \mathbf{K}_1$, in accordance with (2.4). The first assertion now follows from $\mathbf{K}_1 = \mathbf{K}_0K_1$.

With $K_1K_2 = K_3$, $K_2K_1 = K_4$, and $K_1K_2K_1 = K_5$, we obtain further

$$\mathbf{G}K_2 = \mathbf{K}_0K_2 \cup \mathbf{K}_1K_2 = \mathbf{K}_0K_2 \cup \mathbf{K}_0K_1K_2 = \mathbf{K}_2 \cup \mathbf{K}_3,$$
$$\mathbf{G}K_2K_1 = \mathbf{K}_0K_2K_1 \cup \mathbf{K}_0K_1K_2K_1 = \mathbf{K}_4 \cup \mathbf{K}_5.$$

The three sets $\mathbf{G}$, $\mathbf{G}K_2$, and $\mathbf{G}K_2K_1$ are disjoint. Hence they make up a decomposition of $\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}])$ into the subgroup $\mathbf{G}$ and its right cosets with respect to K_2 and K_2K_1 (these are also representatives of the left cosets). It follows that $[\mathrm{SL}(2,\mathbb{Z}[\mathrm{i}]) : \mathbf{G}] = 3$.

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press

However, **G** is not a normal subgroup, for otherwise the factor group would be the cyclic group of order 3, and $(K_2K_1)K_2 = \left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right)$ would have been an element of **G**, which is not true. ∎

Actually $\mathrm{SL}(2, \mathbb{Z}[\mathrm{i}])$ does not have normal subgroups of index 3 at all [2, Proposition 1].

References

[1] A. Baker, *Matrix groups. An introduction to Lie group theory.* Springer-Verlag, London, 2002. http://dx.doi.org/10.1007/978-1-4471-0183-3

[2] B. Fine and M. Newman, *The normal subgroup structure of the Picard group*. Trans. Amer. Math. Soc. **302**(1987), no. 2, 769–786. http://dx.doi.org/10.1090/S0002-9947-1987-0891646-3

[3] H. Goldstein, *Classical mechanics*. 2nd edition. Addison-Wesley, Reading, MA, 1980.

[4] G. Jensen and C. Pommerenke, *Discrete space-time and Lorentz transformations*. Canad Math. Bull. **59**(2016), no. 2, 123–135. http://dx.doi.org/10.4153/CMB-2015-066-4

[5] M. Lorente and P. Kramer, *Representations of the discrete inhomogeneous Lorentz group and Dirac wave equation on the lattice*. J. Phys. A **32**(1999), 2481–2497. http://dx.doi.org/10.1088/0305-4470/32/12/019

[6] J. D. Louck, *A new parametrization and all integral realizations of the Lorentz group*. J. Math. Phys. **43**(2002), no. 10, 5108–5134. http://dx.doi.org/10.1063/1.1505124

[7] R. Penrose and W. Rindler, *Spinors and space-time*. Volume I. Cambridge University Press, Cambridge, 1984. http://dx.doi.org/10.1017/CBO9780511564048

[8] A. Schild, *Discrete space-time and integral Lorentz transformations*. Canad. J. Math. **1**(1949), 29–47. http://dx.doi.org/10.4153/CJM-1949-003-4

Sensburger Allee 22 a, D–14055 Berlin
e-mail: cg.jensen@arcor.de

Institut für Mathematik, Technische Universität, D–10623 Berlin
e-mail: pommeren@math.tu-berlin.de

https://doi.org/10.4153/CMB-2016-084-8 Published online by Cambridge University Press